Ernest F. Koschineg
(*pro hac vice pending*)
Jill H. Fertel
(*pro hac vice pending*)
CIPRIANI & WERNER, PC
450 Sentry Parkway, Suite 200
Blue Bell, PA 19422
ekoschineg@c-wlaw.com
jfertel@c-wlaw.com

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETS

ACE AMERICAN INSURANCE COMPANY & ILLINOIS UNION INSURANCE COMPANY, Plaintiffs, vs. PROGRESS SOFTWARE CORPORATION, Defendant.	Case No.: 1:24-cv-10140 **COMPLAINT**

Plaintiffs Illinois Union Insurance Company ("Illinois Union") and Ace American Insurance Company ("Ace American") (collectively hereinafter "Plaintiffs") by and through its undersigned counsel, Cipriani & Werner P.C., as for its complaint herein, alleges the following upon information and belief.

THE PARTIES

1. Plaintiff Illinois Union Insurance Company a/s/o CBIZ, Inc. ("CBIZ"), is a corporation organized under the laws of Illinois with its principal place of business located in Pennsylvania.

2. At all times material to the Complaint, Illinois Union was licensed to issue insurance policies throughout the United States.

3. Plaintiff Ace American Insurance Company a/s/o Firstsun Capital Bancorp ("Firstsun"), is a corporation organized under the laws of Pennsylvania with its principal place of business located in New Jersey.

4. At all times material to this Complaint, Ace American was licensed to issue insurance policies throughout the United States.

5. Progress Software Corporation (hereinafter "Progress" or "Defendant") is a corporation organized under the laws of Delaware with its principal place of business located at 14 Oak Park Dr. in Bedford, Massachusetts.

6. Progress is a software corporation in the business of creating and deploying business applications. Progress published an annual revenue of 602 million dollars in 2022, representing 13.31% growth from 2021.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. 1332 as the parties are residents of different states and the amount in controversy exceeds $75,000.

8. Venue is proper pursuant to 28 U.S.C. 1391 in that the Defendant's principal place of business is within the District of Massachusetts and is subject to personal jurisdiction within this district.

THE MARKETING OF MOVEit FILE TRANSFER SOFTWARE AS A SECURE FILE TRANSFER SYSTEM

9. Progress identifies itself as a corporation that "develops, markets and distributes software to simplify and accelerate the development, deployment, integration and management of business applications … to deliver superior software products and services that empower partners and customers to dramatically improve their development, deployment, integration and management of quality applications worldwide."[1]

10. Progress's business software applications include several "secure" file transfer programs. Progress advertises these applications as "Secure File Transfer – Essential Security for Your Most Important Files."[2]

11. Progress further advises "[i]n a world built on distributed work and collaboration, securing sensitive files is essential. Progress offers file transfer solutions that secure and encrypt your sensitive files, offer new levels of operational efficiency and meet the compliance standards that meet the compliance standards that matter most to your organization."[3]

12. To that end, Progress offers two purportedly secure file transfer applications- WS_FTP Server & Client ("WS_FTP") and MOVEit Managed File Transfer ("MOVEit").

13. At all times material to this Complaint, Progress marketed WS_FTP and MOVEit as secure file transfer applications that would protect sensitive information from harm.

14. Per Progress, "MOVEit enables your organization to meet strict cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2, and more. Provide a secure

---

[1] Progress Software Corporation, SEC Form 10-K, 2003, available at https://www.sec.gov/Archives/edgar/data/876167/000095013503001256/b45503pse10vk.htm#001 (last accessed October 10, 2023)

[2] https://www.progress.com/file-transfer (last accessed October 10, 2023)

[3] *Id*.

environment for your most sensitive files, while easily ensuring the reliability of core business processes."

15. CBIZ and Firstsun (collectively hereinafter "the Insureds") reasonably relied upon Progress's representations and assurances that MOVEit would adequately secure and encrypt its files, "meet strict cybersecurity compliance standards" and "[p]rovide a secure environment for [their] most sensitive files[.]"

16. At all times material to this Complaint, Ace American provided cyber insurance coverage to Firstsun pursuant to insurance policy D9488634A.

17. This policy specifically provides that Firstsun shall transfer any applicable rights of recovery to Ace American in the event that Illinois Union is caused to make payment under its policy.

18. At all times material to this Complaint, Illinois Union provided cyber insurance coverage to CBIZ pursuant to insurance policy F14973205.

19. This policy specifically provides that CBIZ shall transfer any applicable rights of recovery to Illinois Union in the event that Illinois Union is caused to make payment under its policy.

20. At all times material to this Complaint, Progress maintained a Software License and Maintenance Agreement "the Agreement" with its clients, including but not limited to Firstsun, and CBIZ.

21. In the Agreement, Progress specifies, in pertinent part:

> 9.1 Each party agrees to hold as confidential all Confidential Information received by such party ("Recipient") from the other party ("Disclosing Party")
>
> 9.2 Recipient will use the same care and discretion to avoid disclosure of Confidential Information as it uses with its own

> similar information that it does not wish to be disclosed, *but in no event less than a reasonable standard of care for the industry and materials in question*.

(emphasis added)

THE MOVEit DATA BREACH

22. On or about May 31, 2023, Progress announced a critical vulnerability in its MOVEit Web Application. This vulnerability, identified as CVE-2023-34362, facilitated an SQL injection vulnerability which led to a remote code execution by malicious actors.

23. On that same day, May 31, 2023, Progress offered a software update, or "patch," purportedly rectifying CVE-2023-34362.

24. Though it is unclear when Progress learned of this vulnerability in MOVEit's code, upon information and belief, it is now known that this vulnerability existed within MOVEit's code for at least *two years* prior to disclosure.

25. More importantly, the disclosure of the vulnerability was made several days *after* Russian-based Cl0p ransomware gang ("Cl0p") utilized this vulnerability to access and steal files stored on MOVEit's server.

26. The MOVEit data breach is believed to have impacted at least 383 entities including numerous corporate and government offices, representing the personal information of an astonishing estimated 20,421,414 individuals.

27. This personal information included personally identifiable information ("PII") including but not limited to Social Security numbers, dates of birth, passport information, financial account information, employment authorization card information, addresses, and phone numbers; as well as protected health information ("PHI") such as medical information, diagnostic information, diagnostic codes, treatment codes, diagnostic codes, and medical billing and insurance information.

28. The MOVEit data breach has created astounding financial repercussions for Progress's customers as well as the various companies who relied on Progress's customers and entrusted their personal information to Progress through MOVEit.

29. These costs include forensic investigation, breach notifications, remediations, and ransom demands.

30. As a result of the MOVEit data breach, CBIZ has been forced to expend more than ten million dollars in costs associated with the breach response. These costs are expected to increase.

31. As a result of the MOVEit data breach, Firstsun has been forced to expend more than two million dollars in costs associated with the breach response. These costs are expected to increase.

32. CBIZ and Firstsun have and will be forced to expend monies for forensic investigation, breach notifications, legal costs and remediation.

33. Pursuant to the terms of its cyber insurance policy, Illinois Union was obligated to make a payment in the amount of 5,000,000.00 to CBIZ in response to expenses directly resulting from the MOVEit data breach.

34. Pursuant to the terms of its cyber insurance policy, as of this writing Ace American has been obligated to make payment in the amount of $1,573,949.58 to Firstsun in response to expenses directly resulting from the MOVEit data breach. Upon information and belief, Ace American will be obligated to make addition payments in accordance with this policy.

35. Cl0p is expected to amass between $75-100 million dollars solely from ransomware payments related to the MOVEit data breach.[4]

36. While Ace American, Illinois Union, and the Insureds have been forced to expend millions of dollars in response to the MOVEit data breach, Progress has suffered shockingly minor expenses in comparison. Progress has reported "minimal" financial impact as a result of the MOVEit data breach- an estimated $951,000 in cyber incident and vulnerability response expense- a fraction of its overall revenue.[5]

37. Even after the public disclosure of the SQL vulnerability injection and the massive damage their product has allowed, Progress continues to report financial gains, having reported revenue of $175 million increased 16% year-over-year on an actual currency basis and 14% on a constant currency basis for the third quarter of 2023.

38. Progress promotes their financial growth and recognizes the benefit of financial gain, including that conferred upon it by Plaintiffs and Insureds. According to Progress's Chief Financial Officer, Anthony Folger, Progress is "…very happy with our Q2 results, which again were driven by strong top line performance across virtually all products. Operating margins finished well ahead of our expectations – a reflection of solid execution from our sales teams as well as our integration and operations teams. ARR grew 19% in constant currency to over $569M."[6]

39. In contrast, the estimated financial impact the MOVEit breach is already measuring in the billions based on disclosures filed with state attorneys general and the Securities and

[4] https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/
[5] https://www.cybersecuritydive.com/news/progress-minimal-impact-moveit-attacks/695076/
[6] https://investors.progress.com/news-releases/news-release-details/progress-announces-second-quarter-2023-financial-results (Last visited on October 13, 2023)

Exchange Commission.[7] Based on the number of victims identified and confirmed to be impacted by the breach, the cost of the MOVEit failure is estimated to be $10,637,147,400.00.[8]

40. Thus, while Progress bears the sole responsibility for the vulnerabilities in its systems, it has not borne the costs of the crisis it created. Equity demands otherwise.

SQL INJECTION VULNERABILITIES ARE WELL UNDERSTOOD AND EASILY PREVENTED

41. Structured Query Language (SQL) injection is a well-known attack technique. In 2008, the Cybersecurity and Infrastructure Security Agency ("CISA") issued a bulletin in response to a dramatic increase in SQL injection attacks, advising that detection can be difficult, therefore "[p]revention is the best approach."[9]

42. CISA has advised of the following mitigation recommendations and best practices:

Network Level Recommendations

- Deny access to the internet except through proxies for Store and Enterprise Servers and workstations.
- Implement firewall rules to block or restrict internet and intranet access for database systems.
- Implement firewall rules to block known malicious IP addresses.
- Harden internal systems against the potential threat posed by a compromised system on the local network. (Do not rely on firewalls to prevent access to insecure systems; secure them.)

System/Application Level Recommendations

- Secure both the operation system and the application
    - Consider using NIST or other industry standard security checklists to harden both the operating systems and the applications
    - Run only the minimum required applications and services on servers necessary to perform their intended function. In other words, disable all unnecessary applications and services.

---

[7] https://www.cybersecuritydive.com/news/moveit-attacks-bad-to-worse/690267/#:~:text=Based%20on%20disclosures%20filed%20with,%246.5%20billion%2C%20according%20to%20Emsisoft. (Last visited on October 13, 2023)

[8] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (Last visited on October 13, 2023)

[9] https://www.cisa.gov/sites/default/files/publications/sql200901.pdf (last accessed October 10, 2023)

    - Follow application vendor security and guidelines.
- Update and patch production servers regularly.
    - Include both operating system patches and application patches.
- Disable potentially harmful SQL stored procedure calls.
    - 'xp_cmdshell' on MSSQL has been frequently used by attacker.
- Deny extended URLs.
    - Excessively long URLs can be sent to Microsoft IIS servers, causing the server to fail to log the complete request. Unless specific applications require long URLs, set a limit of 2048 characters. Microsoft IIS will process requests over 4096 bytes long, but will not place the contents of the request in the log files. This has become an effective way to evade detection while performing attacks.
- Sanitize/validate input.
    - Ensure data is properly typed.
    - Ensure data does not contain escaped code.
    - Consider using type-safe stored procedures/prepared statements.
- Ensure error messages are generic and do not expose too much information.
    - Keep error messages short and usable.
    - Do not disclose internal database structure, table names, or account names.
- Use principles of least privilege.
    - Install and run authorized Microsoft SQL Server and IIS services under a non-privileged account.
    - Apply the principal of 'least privilege' on all SQL machine accounts.
    - Remove guest accounts unless operationally necessary.
    - Use an application account for database access.
- Enforce best practice password and account policies.
    - Require the use of a password on Microsoft SQL Server administrator, user, and machine accounts.
    - Change default/built-in account passwords.
    - Chane application account passwords regularly.
    - Use strong passwords.
    - Lock out accounts after several unsuccessful logon attempts.
- Document all database accounts, stored procedures, and prepared statements along with their uses.
    - Delete/disable unnecessary accounts (including default accounts).
    - Delete/disable unnecessary stored procedures/prepared statements.
- Perform regular audits and penetration testing.
    - Audit transaction logs for suspicious activity.
    - Audit group and role memberships to ensure enforcement of least access principles.
    - Audit stored procedures on a regular basis and remove unnecessary ones.
    - If you use ASP, consider using Microsoft's code analyzer.
    - Consider using HP's scrawlr utility to help identify problems.
    - Conduct penetration tests against applications, servers, and perimeter security.[10]

[10] https://www.cisa.gov/sites/default/files/publications/sql200901.pdf (last accessed October 10, 2023)

43. "Simply stated, SQL injection vulnerabilities are caused by software applications that accept data from an untrusted source (internet users), fail to properly validate and sanitize the data, and subsequently use that data to dynamically fail to properly validate and sanitize the data, and subsequently use that data to dynamically construct an SQL query to the database backing that application."[11]

44. It is important to recognize that any data that is passed from the user to the vulnerable web application and then processed by the supporting database represents a potential attack vector for SQL injection."[12]

45. As a software development corporation, Progress was uniquely positioned to prevent SQL injection vulnerabilities. Developers are further advised to employ parameterized rather than dynamic queries. Parameterized queries are simpler to write and understand and prevent the use of SQL commands inserted by an attacker.

46. Additional standard practices to prevent SQL injection vulnerabilities include the use of stored procedures, allow-list input validation, application fuzzing, or the use of web application firewalls.

47. As a software developer, Progress was further in a position to mitigate the risk of SQL injection vulnerabilities by minimizing privileges assigned to each database and employing effective endpoint detection systems.

48. Conversely, the Insureds were not in a position to mitigate or prevent a software vulnerability in MOVEit's code. MOVEit is a closed system; the Insureds could neither access nor control MOVEit's coding. They were not in a position to prevent or detect the flaws in

[11] https://www.cisa.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf (last accessed October 10, 2023)
[12] *Id.*

MOVEit's code, nor could any reasonable security procedure or control allow the Insureds to prevent or mitigate an SQL attack.

49. The Insureds relied upon Progress's misrepresentations regarding the security of their file transfer applications, to their great and continued detriment. Ace American, Illinois Union, and the Insureds have and will continue to suffer continued financial losses as a direct result of Progress's acts, omissions, and misconduct.

50. Concerningly, CVE-2023-34362 was not the only critical vulnerability in MOVEit's code; since the May 31, 2023 announcement, MOVEit has disclosed two additional SQL injection vulnerabilities – CVE-2023-35036 and CVE-2023-35708, each of which would allow a malicious actor to access, modify, and steal data within MOVEit's database.

51. Similarly, on September 27, 2023, cybersecurity researchers announced a maximum severity remote code execution vulnerability in Progress's WS_FTP file share platform.[13] This vulnerability- CVE-2023-40044, a .NET deserialization vulnerability, allows threat actors to remotely execute commands on its operating with a simple HTTP request.[14]

52. On September 30, 2023, cybersecurity company Rapid7 announced that it had observed multiple instances of threat actors exploiting CVE-2023-40044.[15]

53. Progress's response on October 2, 2023- days after the vulnerability was disclosed by a third-party, blamed security researchers for the failures of its code, announcing that it was "disappointed" that security researchers had "provided threat actors a roadmap on how to exploit the vulnerabilities" that Progress itself had created.[16]

---

[13] https://www.bleepingcomputer.com/news/security/exploit-available-for-critical-ws-ftp-bug-exploited-in-attacks/ (last accessed October 10, 2023).
[14] *See Id.*
[15] *See Id.*
[16] *See Id.*

54. Rather than take responsibility for the vulnerability or their lack of disclosure, Progress blamed those who sought to inform their customers. This is particularly concerning given the existence of the MOVEit SQL injection vulnerability for ***two years*** prior to MOVEit data breach.

55. MOVEit's delayed disclosure and/or notification of critical security vulnerabilities prevented its customers, including the Insureds, from taking prompt action, including discontinued use of MOVEit as a "secure" file transfer application. Moreover, this conduct appears to be ongoing.

56. Pursuant to the terms of the subject policy, and otherwise by operation of law, Illinois Union is contractually, legally, and equitably subrogated, to the extent of its payments, to CBIZ's rights against Progress to recover for the amounts paid as a result of the loss, as well as to pursue any uninsured losses suffered by CBIZ by virtue of an assignment of such claims, if any.

57. Pursuant to the terms of the subject policy, and otherwise by operation of law, Ace American is contractually, legally, and equitably subrogated, to the extent of its payments, to Firstsun's rights against Progress to recover for the amounts paid as a result of the loss, as well as to pursue any uninsured losses suffered by Firstsun by virtue of an assignment of such claims, if any.

COUNT I – NEGLIGENCE

58. Plaintiffs incorporate each of the preceding paragraphs and allegations by reference as though fully set forth at length herein.

59. The losses and damages sustained by Plaintiffs and the Insureds were caused by the negligence, gross negligence, carelessness, recklessness, and/or negligent acts and/or

omissions of Progress, its agents, servants, and/or employees acting within the scope of their employment.

60. Progress owed legal and equitable duties to its customers, including the the Insureds, including a duty to adequately design, maintain, and update its software, as well as a duty to promptly detect, repair, and notify of any critical vulnerabilities in its code.

61. Progress failed to use the degree of care which a reasonably prudent software company would use in designing, maintaining, and utilizing a secure file transfer application.

62. Progress's negligent acts and omissions, *inter alia*, include, but are not limited to the following:

a. Negligent design of the MOVEit application;

b. Failure to utilize parameterized inquiries rather than dynamic inquiries;

c. Failure to use stored procedures;

d. Failure to utilize application fuzzing;

e. Failure to use web application firewalls;

f. Failure to provide regular audits and penetration testing;

g. Failure to document all database accounts, stored procedures, and prepared statements along with their uses;

h. Failure to enforce best practice password and account policies;

i. Failure to use principles of least privilege;

j. Failure to ensure that error messages are generic and do not expose to much information;

k. Failure to sanitize and/or validate input;

l. Failure to deny extended URLs;

m. Failure to disable potentially harmful SQL stored procedure calls;

n. Failure to produce proactive patch production or update and patch production servers with regularity;

o. Failure to adequately secure the application and operation system;

p. Failure to deny unnecessary internet access;

q. Failure to block or restrict internet or intranet access for database systems;

r. Failure to implement firewall rules to block or restrict internet and intranet access or implement firewall rules to block known malicious IP addresses; and

s. Failure to harden internal systems against the potential threat posed by a compromised systems against the potential threats poses by a compromised system on their local network.

63. Progress was further negligent in failing to timely detect and remedy the vulnerabilities in MOVEit and to timely provide a software update or patch despite the existence of the vulnerability now known as CVE-2023-34362 for at least two years prior to the MOVEit data breach.

64. A data breach is a foreseeable consequence of failure to adequately design and maintain a file transfer application. Indeed, such consequences have been seen in similar widely publicized breaches, such as the Accellion, Inc. breach, in which over 100 companies, organizations, universities, and government offices were subject to ransomware attacks as a result of vulnerabilities in its system.

65. The highly public nature of the Accellion, Inc. breach and similar breaches placed Progress on notice of the foreseeable consequences to its clients of its failure to adequately design and maintain its application.

66. Moreover, the fact that CVE-2023-34362 existed for at least two years prior to the data breach suggests that Progress, as the developer of MOVEit, knew of the vulnerability. At the very least, Progress should have known of the existence of CVE-2023-34362, or would have known of the vulnerability given reasonably diligent efforts.

67. Despite adequate notice of the risks associated with its failure to adequately design, maintain, and proactively test the MOVEit application, Progress failed to ensure the security of its platform and ultimately the security of its customers' confidential information, including that of the Insureds.

68. As a direct and proximate consequence Progress's misconduct, acts, and omissions, Plaintiffs and the Insureds have experienced direct monetary damages including but not limited to costs associated with ransomware payments, legal fees associated with incident response and regulatory concerns, costs associated with data breach response and forensic investigation, and costs associated with breach remediation.

69. As a direct and proximate consequence Progress's negligent, grossly negligence, and/or reckless conduct, Plaintiffs and the Insureds have experienced and will continue to experience legal jeopardy including but not limited to costs incurred in defending pending and future litigation, including but not limited to filing fees, legal fees, costs related to expert witnesses, fees and costs related to discovery and maintenance of electronically stored information, and costs related to settlement or potentially awarded after an adverse verdict,

70. But for Progress's negligent, grossly negligence, and/or reckless conduct, Plaintiffs and the Insureds would not have experienced these current and future damages.

71. Pursuant to the terms and conditions of its cyber insurance policies, Plaintiffs have paid and will continue to pay funds to or on behalf of the Insureds in an amount to be proven at trial.

72. Pursuant to the terms of the subject cyber insurance policies, and otherwise by operation of law, Plaintiffs are contractually, legally, and equitably subrogated, and has further been assigned the Insureds' rights against Progress to recover damages incurred as a result of the MOVEit data breach.

COUNT II – BREACH OF CONTRACT

73. Plaintiffs incorporate each of the preceding paragraphs and allegations by reference as though fully set forth at length herein.

74. Pursuant to the Agreement, Progress was obligated to treat all information received by its customers, including the Insureds, as Confidential Information.

75. Progress further agreed to use reasonable care and discretion to avoid disclosure of such Confidential Information and further agreed that it would employ "a reasonable standard of care for the industry and materials in question."

76. By failing to employ reasonable industry standards related to prevention of SQL injection vulnerabilities, Progress failed to use reasonable care or employ a reasonable industry standard of care for materials containing PII and PHI.

77. Progress's failure to employ reasonable care and discretion and/or employ a reasonable industry standard of care includes, but is not limited to:

a. Negligent design of the MOVEit application;

b. Failure to utilize parameterized inquiries rather than dynamic inquiries;

c. Failure to use stored procedures;

d. Failure to utilize application fuzzing;

e. Failure to use web application firewalls;

f. Failure to provide regular audits and penetration testing;

g. Failure to document all database accounts, stored procedures, and prepared statements along with their uses;

h. Failure to enforce best practice password and account policies;

i. Failure to use principles of least privilege;

j. Failure to ensure that error messages are generic and do not expose to much information;

k. Failure to sanitize and/or validate input;

l. Failure to deny extended URLs;

m. Failure to disable potentially harmful SQL stored procedure calls;

n. Failure to produce proactive patch production or update and patch production servers with regularity;

o. Failure to adequately secure the application and operation system;

p. Failure to deny unnecessary internet access;

q. Failure to block or restrict internet or intranet access for database systems;

r. Failure to implement firewall rules to block or restrict internet and intranet access or implement firewall rules to block known malicious IP addresses; and

s. Failure to harden internal systems against the potential threat posed by a compromised systems against the potential threats poses by a compromised system on their local network.

78. Progress further failed to comply with reasonable industry standards or reasonable care by failing to timely detect and remedy the vulnerabilities in MOVEit and to timely provide a software update or patch despite the existence of the vulnerability now known as CVE-2023-34362 for at least two years prior to the MOVEit data breach.

79. Accordingly, Progress breached its contractual obligation to ensure confidentiality of Confidential Information belonging to the Insureds

80. As a direct and proximate consequence Progress's breach of the Agreement, Plaintiffs and the Insureds have experienced direct monetary damages including but not limited to costs associated with ransomware payments, legal fees associated with incident response and regulatory concerns, costs associated with data breach response and forensic investigation, and costs associated with breach remediation.

81. As a direct and proximate consequence Progress's breach of the Agreement, Plaintiffs and the Insureds have experienced and will continue to experience legal jeopardy including but not limited to costs incurred in defending pending and future litigation, including but not limited to filing fees, legal fees, costs related to expert witnesses, fees and costs related to discovery and maintenance of electronically stored information, and costs related to settlement or potentially awarded after an adverse verdict.

82. But for Progress's breach of the Agreement, Plaintiffs and the Insureds would not have experienced these current and future damages.

83. Pursuant to the terms and conditions of its cyber insurance policies, Plaintiffs have paid and will continue to pay funds to or on behalf of the Insureds in an amount to be proven at trial.

COUNT III – NEGLIGENT MISREPRESENTATION

84. Plaintiffs incorporate each of the preceding paragraphs and allegations by reference as though fully set forth at length herein.

85. As set forth herein, Progress advertises MOVEit as a *secure* file transfer platform- specifically stating "Secure File Transfer – Essential Security for Your Most Important Files."[17]

86. With respect to its file transfer platforms, including MOVEit, Progress advises "[i]n a world built on distributed work and collaboration, securing sensitive files is essential. Progress offers file transfer solutions that secure and encrypt your sensitive files, offer new levels of operational efficiency and meet the compliance standards that meet the compliance standards that matter most to your organization."[18]

87. Progress therefore marketed MOVEit as secure file transfer applications that would protect sensitive information from harm.

88. Per Progress, "MOVEit enables your organization to meet strict cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2, and more. Provide a secure environment for your most sensitive files, while easily ensuring the reliability of core business processes."

89. The Insureds reasonably relied on the statements made by Progress regarding MOVEit's supposedly secure platform.

90. As demonstrated by the *massive* damage caused by the MOVEit data breach, MOVEit did not provide "essential security" for the Insureds' most confidential documents.

---

[17] https://www.progress.com/file-transfer (last accessed October 10, 2023)
[18] *Id.*

91. Further, as evidenced by the MOVEit data breach, MOVEit did not adequately secure or encrypt information belonging to the Insureds, nor did it "meet the compliance standards that meet the compliance standards that matter most" to the Insureds.

92. Progress knew or should have known that the statements identified herein were false and misleading, based on its subpar database development, security procedures, and controls.

93. The Insureds were harmed by their justifiable reliance upon Progress's fraudulent, reckless, and/or negligent misrepresentation.

94. The Insureds' reliance on Progress's fraudulent, reckless, and/or negligent misrepresentation was a substantial factor in causing the harm that they sustained.

95. As a direct and proximate consequence of Progress's fraudulent, reckless, and/or negligent misrepresentation Plaintiffs and the Insureds have experienced direct monetary damages including but not limited to costs associated with ransomware payments, legal fees associated with incident response and regulatory concerns, costs associated with data breach response and forensic investigation, and costs associated with breach remediation.

96. As a direct and proximate consequence of Progress's fraudulent, reckless, and/or negligent misrepresentation, Plaintiffs and the Insureds have experienced and will continue to experience legal jeopardy including but not limited to costs incurred in defending pending and future litigation, including but not limited to filing fees, legal fees, costs related to expert witnesses, fees and costs related to discovery and maintenance of electronically stored information, and costs related to settlement or potentially awarded after an adverse verdict,

97. But for Progress's negligent misrepresentations, Plaintiffs and the Insureds would not have experienced these current and future damages.

98. Pursuant to the terms and conditions of its cyber insurance policies, Plaintiffs have paid and will continue to pay funds to or on behalf of the Insureds in an amount to be proven at trial.

COUNT IV – PRODUCTS LIABILITY: PRODUCT DESIGN DEFECT

99. Plaintiffs incorporate each of the preceding paragraphs and allegations by reference as though fully set forth at length herein.

100. Progress is in the business of selling software.

101. MOVEit is a product designed, sold by, and placed into commerce by Progress.

102. Progress expected MOVEit to reach the seller without substantial change; moreover, MOVEit reached its consumers without change, upon information and belief.

103. MOVEit is unreasonably dangerous as designed in that it:

a. Failed to utilize parameterized inquiries rather than dynamic inquiries;

b. Failed to use stored procedures;

c. Failed to utilize application fuzzing;

d. Failed to use web application firewalls;

e. Failed to provide regular audits and penetration testing;

f. Failed to document all database accounts, stored procedures, and prepared statements along with their uses;

g. Failed to enforce best practice password and account policies;

h. Failed to use principles of least privilege;

i. Failed to ensure that error messages are generic and do not expose to much information;

j. Failed to sanitize and/or validate input;

k. Failed to deny extended URLs;

l. Failed to disable potentially harmful SQL stored procedure calls;

m. Failed to produce proactive patch production or update and patch production servers with regularity;

n. Failed to adequately secure the application and operation system;

o. Failed to deny unnecessary internet access;

p. Failed to block or restrict internet or intranet access for database systems; and

q. Failed to implement firewall rules to block or restrict internet and intranet access or implement firewall rules to block known malicious IP addresses;

104. As a result of these multiple design failures, MOVEit, advertised as a secure file transfer platform, was effectively a trojan horse, allowing Cl0p- a notorious international ransomware unfettered access to the most confidential of data belonging to Progress's customers, including the Insureds.

105. But for the numerous design defects in MOVEit's code, Cl0p would never have had access to confidential information belonging to the Insureds.

106. In our data driven economy, an insecure secure file transfer platform is an inherently dangerous product.

107. Applying a risk-utility analysis, the utility of a supposedly secure file transfer platform is dramatically outweighed by the demonstrated lack of adequate security provided by MOVEit.

108. MOVEit was in defective condition and unreasonably dangerous when it left Progress's control.

109. MOVEit, as sold and licensed by Progress, was at all times material to this Complaint, in a condition not contemplated by the ordinary consumer which was unreasonably dangerous.

110. Progress did not provide adequate warning as to the dangers and inadequacies of its MOVEit platform.

111. The defect in MOVEit's design was the proximate cause of the damages sustained by Plaintiffs and the Insureds as described herein.

112. In fact, the mere showing of the MOVEit data breach evidences its defective condition.

113. As a direct and proximate consequence of MOVEit's defective and unsafe design, Plaintiffs and the Insureds have experienced direct monetary damages including but not limited to costs associated with ransomware payments, legal fees associated with incident response and regulatory concerns, costs associated with data breach response and forensic investigation, and costs associated with breach remediation.

114. As a direct and proximate consequence of MOVEit's defective and unsafe design, Plaintiffs and the Insureds have experienced and will continue to experience legal jeopardy including but not limited to costs incurred in defending pending and future litigation, including but not limited to filing fees, legal fees, costs related to expert witnesses, fees and costs related to discovery and maintenance of electronically stored information, and costs related to settlement or potentially awarded after an adverse verdict,

115. But for MOVEit's defective and unsafe design, Plaintiffs and the Insureds would not have experienced these current and future damages.

116. Pursuant to the terms and conditions of its cyber insurance policies, Plaintiffs have paid and will continue to pay funds to or on behalf of the Insureds in an amount to be proven at trial.

COUNT V – UNJUST ENRICHMENT

117. Plaintiffs incorporate each of the preceding paragraphs and allegations by reference as though fully set forth at length herein.

118. Plaintiffs bring this claim in addition to or in the alternative to its claim for breach of contract as Plaintiffs may not have an adequate remedy at law against Progress.

119. Plaintiffs and the Insureds have both an equitable and legal interest in the protection and security of sensitive data of the Insureds, bargained for via the product expressly offered by Progress through the purchase and use of MOVEit secure file transfer software designed to "provide a secure environment for your most sensitive files".[19]

120. In offering MOVEit to Chubb Insureds, Progress understands Chubb Insureds' "business depends on transferring mission critical, sensitive data securely and reliably". Progress promised "MOVEit is a proven enterprise class, secure, file transfer solution to get your files where they need to go" and that "MOVEit keeps your files secure both in transit and at rest with a tamper evident audit log" to prove regulation compliance while simultaneously "maintaining complete visibility and control over file transfer activities between partners, customers, users, and systems."[20]

121. Progress expressly promised -- and continues to promise -- that MOVEit software will "meet strict cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2 and

[19] https://www.progress.com/moveit (last visited October 17, 2023)
[20] https://youtu.be/Mpan_9u9f0M via https://www.progress.com/moveit (both last visited October 13, 2023)

more…[by providing] a secure environment for your most sensitive files, while easily ensuring the reliability of core business processes".[21]

122. Progress further promised use of its MOVEit software would save the Insureds money, promising that "MOVEit lets you lower operational costs by consolidating all of your file transfer activities to one scalable system."[22]

123. Progress contemplated the importance and necessity of transparency for the Insureds by promising MOVEit "dashboards make it easy to see the status and performance of your transfers in real time and at a glance…[and provide the] data transfer audit trails [the Insureds] need."[23]

124. Progress holds itself out publicly as a trustworthy industry leader worldwide by advertising that customers, including the Insureds, should "trust Progress for innovation and results" and claims that "top 10 tech companies rely on Progress", "the 30 largest companies in the world trust Progress" and "70% of Fortune 500 companies trust Progress."[24]

125. MOVEit has been so successfully marketed and sold as a necessary, safe, and reliable product to protect data that Progress promotes MOVEit's use in the healthcare industry as well as by thousands of IT departments in high technology, government, and financial service companies.

126. Wholly unaware of the dangers MOVEit software posed, the Insureds conferred a benefit upon Progress in the form of financial payment for Progress's product: MOVEit managed file transfer software.

---

[21] https://www.progress.com/moveit (last visited October 13, 2023)
[22] Id.
[23] Id
[24] https://www.progress.com/ (last visited October 17, 2023)

127. Progress had knowledge of the financial benefit of payment by the Insureds for the use of MOVEit and voluntarily accepted payment.

128. Progress benefited and continues to benefit from the funds paid by, and accepted from, the Insureds.

129. MOVEit was made available for purchase at all times related to this action and Chubb's Insureds purchased and used MOVEit as advertised and instructed.

130. The Insureds relied upon Progress's misrepresentations regarding the security of their file transfer applications, to their great and continued detriment. Plaintiffs and the Insureds have and will continue to suffer continued financial losses as a direct result of Progress's acts, omissions, and misconduct.

131. At all times material to this Complaint, MOVEit was falsely marketed as safe and sold with a dangerous SQL vulnerability – Progress's reported financial growth year after year.

132. Progress failed to provide the safety and security the Insureds bargained for resulting in injury and damages to the same.

133. But for Progress's guarantees that MOVEit would provide protection against the exact damage it instead exposed and inflicted upon Plaintiffs and the Insureds, MOVEit would not have been purchased, used, and/or trusted by the Insureds.

134. But for the reliance upon Progress's representations of their products safety and security, Plaintiffs and the Insureds would not have been exposed to the ongoing injury and damage resulting from the breach of Progress's MOVEit file transfer software.

135. Progress failed to expend the necessary funds to ensure the product they designed, created, marketed, maintained, and distributed was safe and providing all guarantees made and relied upon by the Insureds.

136. Progress continues to financially benefit from and by continued possession of the monies paid by Plaintiffs and the Insureds and all others similarly situated. Progress has been and will continue to be unjustly enriched by maintaining the funds received without providing the services and products bargained for. Retention of the funds paid to Progress for MOVEit by Plaintiffs and the Insureds would be unjust under the circumstances.

137. But for Progress's willingness and commitment to maintain the security, privacy, and confidentiality of data by and within MOVEit, Plaintiffs and the Insureds would not have provided or authorized data to be provided to Progress's MOVEit, and Progress would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining clients, gaining the reputational advantages conferred upon it by Plaintiffs and the Insureds, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

138. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs and the Insureds and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the data and information belonging to the Insureds without having adequate data security measures; and its other conduct facilitating the theft of data and information, Progress has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Insureds.

139. Progress's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of the Insureds' sensitive data and information, while at the same time failing to maintain that information secure from intrusion.

140. Under the common law doctrine of unjust enrichment, it is inequitable for Progress to be permitted to retain the benefits it received, and is still receiving, without justification, from the Insureds in an unfair and unconscionable manner. Progress's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

141. Plaintiffs a/s/o the Insureds are entitled to full refunds, restitution, and/or damages from Progress and/r an order proportionally disgorging all profits, benefits, and other compensation obtained by Progress from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiffs and the Insureds can seek restitution or compensation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Illinois Union Insurance Company a/s/o CBIZ, Inc. and Ace American Insurance Company a/s/o Firstsun Capital Bancorp respectfully demand judgment be entered in their favor and against Defendant Progress Software Corporation for:

- money damages in an amount to be proven at trial
- a declaration by this Court that, in the event of any judgment against the Insureds in favor of a plaintiff or putative class, that:
    - Progress is liable to any such plaintiff or class over the Insureds;
    - Progress is liable to the Insureds by common law indemnity; and
    - Progress is liable to the Insureds by way of contribution
- reasonable costs and attorneys' fees;

- Pre and post judgment interest; and,
- Any such further relief as this Honorable Court deems just and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury.

Dated: January 18, 2024

For the Plaintiffs,

/s/ Ernest F. Koschineg
Ernest F. Koschineg
(*pro hac vice pending*)
Jill H. Fertel
(*pro hac vice pending*)
CIPRIANI & WERNER, PC
450 Sentry Parkway, Suite 200
Blue Bell, PA 19422
(610) 567-0700
ekoschineg@c-wlaw.com
jfertel@c-wlaw.com

/s/ Brian J. Palmeri
Brian Palmeri (BBO No. 568823)
Winget, Spadafora & Schwartzberg, LLP
One Boston Place, Suite 2600
Boston, MA 02108
(617) 544-9900
palmeri.b@wssllp.com